UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
the person of Gurtej Singh and any computers or digital devices located thereon

Case No. 2:22-mj-378

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment B, incorporated herein by reference

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment C, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sec. 659	Theft from Interstate Shipment
18 U.S.C. Sec 1001	Knowingly making a materially false statement or representation
18 U.S.C. Secs 1343 & 1349	Wire fraud and conspiracy to commit wire fraud

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

BILAL TEMSAH Digitally signed by BILAL TEMSAH Date: 2022.05.23 20:41:14 -04'00'

Applicant's signature

Bilal Temsah, SA U.S. DOT-OIG

Printed name and title

Sworn to before me and signed in my presence.

VIA AUDIO CALL

Date: May 27, 2022

Judge's signature

City and state: Columbus, OH

Elizabeth A. Preston Deavers U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF Gurtej Singh and the premises located at 3739 and 3743 Interchange Road, Columbus, OH 43204, including any storage vehicles located on the premises, and any computers or digital devices located thereon/therein	**Case No.** _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Bilal Temsah, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search Gurtej Singh and the premises known as 3739 and 3743 Interchange Road, Columbus, OH 43204, hereinafter "PREMISES," further described in Attachments A and B, for the things described in Attachment C.

2. I am a Special Agent with the United States Department of Transportation (USDOT), Office of Inspector General (OIG), in Columbus, Ohio. I have been employed as a USDOT-OIG Special Agent for approximately three years. I have successfully completed criminal investigator training at the Federal Law Enforcement Training Center in Glynco, Georgia. As a Special Agent, I conduct criminal investigations of individuals and entities for possible violations of federal criminal laws, particularly those laws found in Titles 18 and 49 of the U.S. Code that are relevant to the USDOT, Federal Motor Carrier Safety Administration (FMCSA). FMCSA responsibilities include monitoring and enforcing compliance with regulations governing safety and commerce related to interstate motor carriers, in particular Title 49, Code of Federal Regulations. Further, I have specific experience and knowledge

investigating the type of violations set forth below. I have participated in the execution of numerous search warrants at businesses and residences for documents, records, receipts, and computer-related equipment used to store information.

3. The facts set forth in this affidavit are based on my own investigation, which includes my own personal observations and knowledge; interviews of witnesses and potential suspects/targets; documents provided by witnesses; documents and information obtained through search warrants; information from FMCSA database systems; information I have received from other law enforcement officers; and my training and experience. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have not omitted any information that would negate probable cause.

4. The affidavit is submitted in support of an application for a federal search warrant to search the person of Gurtej Singh, aka Gary Singh, aka Gary Bhullar, hereinafter G. Singh, and also the PREMISES, which is the business premises of Bhullar Transport Group LLC (hereinafter known as "Bhullar Transport"). Bhullar Transport is an active Motor Carrier (MC) company authorized to transport property in interstate commerce. G. Singh, who is a target of the investigation, is the owner of Bhullar Transport. From at least the early 2000s, G. Singh also worked for Cargo Solution Express, Inc. ("CSE"). During the existence of CSE, brothers Bobby Kang, Baldev Kang, and Yudvinder Kang (hereinafter collectively known as the Kang brothers), who owned CSE, in addition to G. Singh, have created several other MC companies to circumvent the FMCSA regulations, including 3 Bros LLC, Bal Carrier, Best Carrier, Inc., Cargo Solution Brokerage, Inc., Cargo Solution Georgia, Cargo Solution Express, Cargo Solution Inc., Cargo Solution Ohio, Inc., Kang Carrier and Investments Inc. DBA Rose Express. Because these

entities are generally run as a single business, I refer to them collectively herein as "CSE." Amandeep Singh (hereinafter A. Singh) is another target of this investigation and worked for CSE.

5. Based on the facts set forth below, there is probable cause to believe that on the person of G. Singh and at the PREMISES there exist evidence, fruits, and instrumentalities of 18 U.S.C. §§ 659 (Theft from Interstate Shipment); 1001 (False Statement); 1343 (Wire Fraud); and 1349 (Wire Fraud Conspiracy).

RELEVANT FEDERAL REGULATIONS AND DEFINITIONS

6. The FMCSA is an administration arm of the USDOT responsible for regulating and providing safety oversight of MCs operating commercial motor vehicles (CMVs) in interstate commerce. Its mission is to reduce crashes, injuries, and fatalities involving CMVs and buses. To implement this directive, the FMCSA prescribed safety regulations, 49 C.F.R. Parts 350-399 (hereinafter referenced as the "FMCSA Safety Regulations"). Thus, as a Special Agent with USDOT-OIG, I am familiar with the federal statutes and regulations governing MCs and CMVs. In relevant part, these statutes and regulations provide as follows.

7. All prospective MCs must apply, through the FMCSA, for a USDOT number and MC authority to operate as a MC by filling out an OP-1 form, also known as a Form MCSA-1. *See* 49 C.F.R. § 365.105T; 49 U.S.C. 13902(a); and 49 C.F.R. § 392.9a. On the OP-1 forms, all applicants must disclose, under penalty of perjury, any relationship with any other FMCSA-regulated entity within the past three years, including any ownership interests or management positions. This disclosure aids the FMCSA in fulfilling its safety mission by detecting and preventing deficient and hazardous MCs from operating. Further, MCs must also file a MC Identification Report, also known as Form MCS-150, when filing for a new application and

when updating the USDOT registration, which is required every two years or any time a regulated entity changes its name, address, or other details in its record. 49 C.F.R. § 390.19T.

8. To fulfill its safety mission of reducing crashes, injuries, and fatalities involving CMVs, the FMCSA restricts the Hours of Service (HOS) for CMV drivers in 49 C.F.R. § 395 to prevent fatigued driving, an underlying cause behind fatal CMV crashes. The HOS regulations set the maximum amount of time CMV drivers are permitted to be on duty, including driving time, and specifies the number and length of rest periods, to help ensure that drivers are awake, alert, and not fatigued. The HOS regulations dictate that MCs record and maintain information pertaining to all drivers' duty status, which is frequently referred to as a logbook. Depending on the MC's operation, a logbook may be kept in a paper or Electronic Logging Device (ELD) format. ELDs were created in order to provide a method of documenting drivers' hours that is less susceptible to manipulation or falsification than written logbooks. ELDs connect to a port in the cab of the CMV and obtain information directly from the engine of the CMV regarding when the engine is started, how fast, how far, and how long the CMV has travelled, and when the CMV has stopped. The information obtained translates into a readable logbook format through use of an application on a cellular phone, tablet or similar device. The information created through the application is also generally maintained on the computers or digital devices at the offices of the MC by whom the driver is employed.

9. The HOS regulations dictate that MCs assign a unique ELD username to each CMV driver and ensure that the driver's license number used in the creation of an ELD driver account is valid and corresponds to the respective driver, to prevent HOS falsification. Under the FMCSA HOS regulations, no MC "shall permit or require" any driver to falsify any records of duty status. *See* 49 C.F.R. § 395.8. The FMCSA Safety Regulations also warn that "[a] person

who violates the rules…may be subject to civil or criminal penalties." 49 C.F.R. § 390.37. Although ELDs were created to prevent HOS falsification, some CMVs and MCs have developed methods to attempt to falsify the information reported in ELD logbooks.

10. To further fulfill its safety mission, the FMCSA implemented a safety rating process. A safety rating is an evaluation of a MC's compliance with the safety fitness standard; the process is described in 49 CFR § 385, Appendix B. The FMCSA may issue one of three safety ratings, Satisfactory, Conditional, or Unsatisfactory. A safety rating is issued after a Rated Investigation (Compliance Review). Not all investigations result in a safety rating. A compliance review may be conducted to investigate potential violations of safety regulations or complaints about MCs, among other reasons. Final safety ratings may be used by shippers and consumers to make decisions about which MCs to hire. The FMCSA does not issue safety ratings to drivers, only to MCs. A ***Satisfactory*** *safety rating* means that a MC has functional and adequate safety management controls to meet the safety fitness standard prescribed in 49 CFR § 385.5. A ***Conditional*** *safety rating* means a MC does not have adequate safety management controls in place to ensure compliance with the safety fitness standard, which **could** result in occurrences listed in 49 CFR § 385.5 (a) through (k), such as unsafe vehicles operating on highways; use of fatigued drivers; use of unqualified drivers; and failure to maintain accident registers and copies of accident reports. ***Unsatisfactory*** *safety rating* means a MC does not have adequate safety management controls in place to ensure compliance with the safety fitness standard, which **has** resulted in occurrences listed in 49 CFR § 385.5. Finally, a safety rating of ***Unrated*** means that a safety rating has not been assigned to the MC by the FMCSA.

11. A MC's FMCSA rating can have various impacts on its business. Insurance companies utilize FMCSA safety ratings in setting rates for insurance policies issued to MCs.

Vendors and shipping brokers also utilize these ratings, amongst other information, in determining whether to hire a particular MC. Many shipping contracts are secured through use of shipping brokers – a kind of intermediary between shippers, receivers and MCs – through the use of online portals and email. These brokers maintain "do not use" MC lists, and those lists frequently relate to the MCs' FMCSA safety ratings as well as the MCs' histories of poor customer service and unresolved claims, such as failure to deliver full loads or delivering damaged goods.

PROBABLE CAUSE

12. As set forth below, G. Singh, along with other co-conspirators, operating through CSE, Bhullar Transport and other MCs, has been intentionally engaged in an ongoing scheme to provide falsified records with the intent to impede and obstruct investigations conducted by the FMCSA. Specifically, as early as on or about May 21, 2015, to the present, the scheme has involved providing false information to the USDOT, by misrepresenting the ownership, nature, and history of Bhullar Transport and other MCs. Much of the false information and misleading communications that G. Singh has engaged in occurred via email, online submissions and/or cellular phone calls or text messages.

13. Further, as early as in or about March 2019, G. Singh, along with other co-conspirators, stole property that was part of interstate shipments transported by CSE. G. Singh stored the stolen property at the CSE warehouse located in Columbus, OH.

Background and Summary of Investigation

14. Beginning in June of 2019, the Columbus Police Department (CPD) initiated an investigation into A. Singh when they received information pertaining to A. Singh's sales of Shark vacuums at various pawn shops in the Columbus, Ohio area. Investigation of those sales

revealed that the vacuums were part of an interstate shipment that was designated for delivery to an Amazon warehouse located in Groveport, Ohio. CSE was the MC responsible for the shipment of the vacuums, and A. Singh was an employee of CSE. CSE failed to deliver a total of 308 Shark RV750 vacuums to Amazon, and all of the vacuums were considered stolen.

15. As a result of this information, CPD, USDOT-OIG agents, and other law enforcement interviewed A. Singh and other employees of CSE, conducted a consent search of the Columbus CSE warehouse, and executed search warrants at that warehouse and on several trailers that were located at the warehouse. USDOT-OIG agents have also obtained FMCSA records pertaining to CSE, Bhullar Transport, G. Singh, and other related entities and individuals. The results of these investigative steps are described in detail below.

Bhullar Transport and CSE Affiliation

16. During the investigation, it was revealed that CSE and Bhullar Transport are affiliated companies. For example:

a) FMCSA records revealed that on or about January 11, 2019, G. Singh established Bhullar Transport as an MC by electronically submitting an OP-1 to the FMCSA, and on the OP-1, G. Singh listed his email address as gary@cargosolutionexpress.com. This submission was accompanied by a mandatory $300 electronic payment.

b) According to records obtained from CSE pursuant to the execution of a search warrant (discussed in more detail below), on or about August 26, 2019, an employee of CSE, Padhuman Kalpattu Govindan, completed two Weekly Settlement Statements one for CSE, and the other for Bhullar Transport. The fact that the same employee completed such paperwork for both companies indicates that the two companies were basically operating as one, which indicates that CSE and Bhullar Transport were

involved in a "chameleon" MC scheme. In these schemes, a MC that has an unfavorable rating by the FMCSA and/or a history of unsatisfactory safety ratings, adverse roadside inspections, and/or unfavorable relationships with shippers, vendors, and/or brokers, essentially merges with or disguises itself under another MC that has little or no history and more favorable safety ratings and/or customer relations history. The two MCs utilize many of the same employees, drivers, and CMVs, but operate under different business names and USDOT numbers. In an attempt to detect and prevent such schemes, the FMCSA requires MCs to disclose any relationships with other MCs. In this instance, both CSE, which had a history of poor safety ratings and customer service relations, and Bhullar Transport, which, as a new company, did not have a significant safety rating, inspection history, or customer service history, failed to disclose their relationship to the FMCSA to circumvent the FMCSA's regulations.

c) On August 6, 2020, Maria Singh, a previous employee of CSE, was interviewed by law enforcement and stated that she was hired and paid by CSE but performed duties, such as hiring of drivers and completing drivers' settlements, for other MCs affiliated with CSE, to include Bhullar Transport.

d) On September 22, 2020, one of the Kang brothers, Yudvinder Kang, acknowledged in a statement to law enforcement that G. Singh was affiliated with CSE and owned Bhullar Transport.

e) Further, FMCSA's records showed the same drivers and CMVs operating for both CSE and Bhullar Transport. For example, both CSE and Bhullar Transport shared the following drivers and CMVs:

i. Abdoul Kane, Abdulkadir Osman, Muhadean Al-Shamari, and Gurpreet Singh

ii. CMV VIN numbers: 1GRAP0625ET588692, 1JJV532D1FL879225, 3H3V532C7HT371786, 3H3V532C2JR119012, 1UYVS2533H7086312, 3H3V532CXKT680580, 3H3V532C0KR211852, 3H3V532C8KT680089, 3H3V532C3KT680274, 3H3V532C0KT680832, 1FUJA6CK49DAC5451, and 3H3V532C9KR851168.

Fraudulent Misrepresentations to the USDOT

17. G. Singh has provided false information to the USDOT in service of a "Reincarnated" MC scheme. Generally speaking, much like a chameleon MC scheme, in a reincarnated MC scheme, an existing MC with a history of regulatory violations continues operations under a new name and MC number, effectively giving the company a clean slate. Such a scheme requires concealing from USDOT and the FMCSA the relationship between the old and new MCs. G. Singh used Bhullar Transport in just this way to "reincarnate" existing MCs under his control.

18. Specifically, on or around February 12, 2012, on a form MCS-150 submitted to FMCSA, G. Singh indicated he was the CEO of Show Time Carrier, Inc. On or around December 14, 2012, the FMCSA conducted a compliance review on Show Time Carrier. On or around December 19, 2012, the FMCSA issued a letter to Show Time Carrier which proposed to Show Time Carrier a conditional safety rating as a result of numerous violations discovered during the aforementioned onsite compliance review. As noted, a conditional safety rating means that the MC does not have adequate safety management controls in place to ensure compliance with the FMCSA safety fitness standards. In May of 2013, the FMCSA ordered Show Time

Carrier to cease all interstate transportation and suspended Show Time Carrier's FMCSA registration due to its failure to pay a penalty related to its violations.

19. On or around May 21, 2015, Shaminder K. Dhaliwal, G. Singh's spouse, electronically submitted an OP-1 form to the FMCSA establishing Roadhawk Transport, Inc., in which Dhaliwal was listed as the president of the company.

20. An FMCSA investigation subsequently revealed that G. Singh was managing and operating both Show Time Carrier and Roadhawk Transport at the same time. As a result of FMCSA's determination regarding the interrelated nature of the two companies, on or around April 13, 2016, Dhaliwal, as the president for Roadhawk Transport, and G. Singh, as the president of Show Time Carrier, signed a stipulated order on consent to consolidate and merge the two MCs. On or around April 14, 2016, G. Singh signed an FMCSA form indicating that he was the Vice President of the newly consolidated Roadhawk Transport. The FMCSA subsequently revoked Roadhawk's operating authority on March 01, 2017.

21. On or around July 26, 2017, as part of their routine and required CMV inspections, the Ohio State Highway Patrol, Motor Carrier Enforcement Unit, inspected a CMV bearing Roadhawk Transport's logo and USDOT number. The CMV driver was Abdirashid Habad who also operated CMVs for CSE according to the FMCSA records. This inspection documented that Roadhawk Transport ignored the FMCSA's revocation and continued operating.

22. On or around January 11, 2019, G. Singh electronically submitted an MCSA-1 for Bhullar Transport to the FMCSA. In doing so, G. Singh provided false information. Specifically, G. Singh affirmed that within 3 years of the date of filing the MCSA-1, G. Singh did not have relationships involving common stock, common ownership, common management, common

control, or familial relationships with any other FMCSA-regulated entities. However, as indicated above, in the three-year period preceding his submission of the MCSA-1 for Bhullar Transport, G. Singh was both (a) the vice president of Roadhawk Transport; and (b) a manager for CSE.

23. In addition to the false statement in the Bhullar Transport MCSA-1, G. Singh also directed employees from CSE to falsify their logbooks, and he appears to have facilitated or directed the falsification of logbooks at Bhullar Transport. As discussed above, the FMCSA relies on logbooks, which it requires MCs to maintain for six months, to determine whether MCs are in compliance with HOS rules and regulations.

24. A. Singh reported to law enforcement that G. Singh issued multiple ELD identification codes to Bhullar Transport drivers. This allowed drivers to drive long hours, in violation of HOS rules, while creating false logbooks that gave the appearance of a two-driver team that was complying with HOS rules. A sample of random roadside inspections conducted by various law enforcement agencies nationwide documented Bhullar Transport's drivers' HOS violations, including logbook falsification. The following are additional examples of other kinds of evidence showing how G. Singh, CSE and Bhullar Transport falsified HOS records:

a) Records seized by CPD Detectives during a search warrant executed on September 3, 2019, at the CSE location in Columbus, Ohio, revealed that on November 10, 2017, G. Singh directed, via email, other employees of CSE, including the Kang brothers, to falsify logbook(s) to conceal the actual route taken by the driver in order to deny a vendor's damage claim.

b) On or about March 09, 2021, the Arizona Department of Public Safety, Commercial Vehicle Enforcement Bureau, Report number AZ0294001396, randomly inspected

Gagandeep Singh, a Bhullar Transport driver, and discovered that the driver had falsified his logbooks for seven consecutive days, falsely claiming to have a co-driver. The driver was prohibited from operating on public roads until the discovered violations were corrected. Such a prohibition is known and documented as an Out of Service Order (OOSO).

c) On or about March 30, 2022, the Arizona Department of Public Safety, Commercial Vehicle Enforcement Bureau, Report number AZ0294001847, randomly inspected Gurpreet Singh, a Bhullar Transport driver, and placed the driver on OOSO for falsifying his March 29, 2022, logbook.

Theft from Interstate Shipments

21. The investigation into CSE and G. Singh began in or around June of 2019, when the CPD Pawn Shop Unit Detective J. Gubernath randomly inspected Levs Pawn Shop (Levs) located at 643 Harrisburg Pike, Columbus, OH 43223. Detective (Det.) Gubernath noticed brand new packages for sale at Levs that displayed Amazon logo and Amazon shipping labels. Det. Gubernath found the packages suspicious due to their impeccable condition, and so he provided the shipping information to CPD Det. B. Crawford, who verified with Amazon that the merchandise was ordered but was never delivered to its final destination. Levs provided CPD with records that showed A. Singh sold the undelivered Amazon merchandize to Levs on multiple dates to include March 04, 2019. On August 27, 2019, Det. B. Crawford interviewed A. Singh, who indicated that his supervisor, "Gary," later identified as G. Singh, directed him to sell the merchandize and shared in the profits. Further, A. Singh informed the detectives that there were three additional trailers containing Amazon merchandise at CSE's yard located at 4540 Fisher Rd., Columbus, OH 43228.

25. On August 27, 2019, Detectives from CPD interviewed G. Singh, who identified himself to the detectives as CSE's Terminal Manager. The CPD detectives informed G. Singh that CPD had arrested A. Singh for selling stolen Amazon property to Levs. G. Singh identified A. Singh as his Warehouse Manager. G. Singh confirmed that the trailers A. Singh referenced were located in bays 11, 13, and 21 of the CSE warehouse. After G. Singh consented to a search without a warrant, the detectives verified that the three trailers contained undelivered merchandise. The detectives then impounded the trailers. During the interview, G. Singh noted that the merchandise was refused by the warehouse where the merchandise was supposed to be delivered because the merchandise was damaged. CPD detectives visually observed and communicated to G. Singh that the merchandise packaging did not appear to be damaged. Then, G. Singh changed his story and indicated that two of the semi-trailers were discovered to contain undelivered merchandise when they arrived at CSE's warehouse from the delivery location and noted that the trailers were supposed to be returned empty by the receivers.

26. On or about September 03, 2019, a search warrant was executed at the CSE warehouse at 4540 Fisher Road, Columbus, OH 43228, and law enforcement officers seized approximately $516,171.50 of undelivered property from interstate shipments carried by CSE. The undelivered merchandize belonged to various buyers and shippers, to include Amazon, National Presto, Inc., and L Brands. The merchandize was taken from various shipments that CSE had been contracted to deliver to the buyers in Ohio. The Amazon property included Shark Ion Robot vacuums, which were part of the same shipment as the units A. Singh had sold to Levs, and curved-screen computer monitors, some of which were still in boxes on pallets. Other curved-screen monitors of the exact same make and model as those on the pallets were in use in the CSE warehouse office, however the serial numbers had been removed from the monitors in

the warehouse office so that law enforcement could not confirm whether they had been part of the shipment intended for delivery to Amazon. The L Brands property consisted of 11 pallets of Bath and Body Works product that was supposed to be delivered to the L Brands location in Reynoldsburg, Ohio in December of 2018.

27. Interviews of A. Singh and other CSE employees revealed that the above-described goods were not delivered, in some instances, due to a fraudulent consolidation scheme by G. Singh and CSE. In this scheme, CSE would typically—and unbeknownst to its customers, shippers, and receivers—commingle shipments that were supposed to remain separate; transport the commingled shipments over a long distance; separate out the commingled shipments near their destinations; then deliver the separate shipments as if they had remained separate and never been commingled.

28. For background, it is common practice in the trucking business to add a unique security "seal" to a loaded trailer that will break if the trailer is opened. The seal is generally a piece of plastic or rubber, often imprinted with a unique identification number that is included in the delivery paperwork. When the shipment is delivered, if the seal matches the description in the paperwork and remains intact, the recipient is assured that the trailer was not opened and the content was not compromised while in transit.

29. The scheme carried out by G. Singh and CSE began with CMVs picking up property in sealed trailers and transporting them to a nearby location where CSE employees would breach the security seals on the trailer. This generally happened in one of two ways. Sometimes the seal was simply cut. In many cases, however, CSE employees were able to keep the original seal intact when opening trailers. They accomplished this by flipping the bolts on the locking mechanisms on the trailer doors, which gave the employees access to unscrew the bolts

and remove the entire locking mechanisms from the exterior of the trailer. To do this, CSE employees simply turned the carriage bolts of the clasps around so the carriage bolt head was on the inside of the trailer and the nut of the carriage bolt was on the outside of the trailer. Consequently, to remove the clasps, a wrench was used to remove the nut of the carriage bolt. The entire locking mechanism was then disassembled from the exterior of the trailer, keeping the seal intact.

30. At this point, various loads from various shippers were commingled and consolidated into one or more trailers. The commingled loads were then transported to another CSE location closer to the destination. There, the loads were then separated back to their original configurations. By commingling loads, CSE reduced the number of CMVs and trailers that had to make long journeys, thereby reduced its operating costs, and increased its profit.

31. Just before delivery, a new seal was placed on the trailer doors (if the original had been cut), or the locking mechanism with the original seal was reattached. The bill of ladings, if necessary, would then be altered to reflect the new seal number(s) (for cut seals) and the new trailer numbers (because some of the original trailers did not make the journey). This made it appear as if the trailers were never opened while in CSE's possession.

32. During the commingling and separating of loads, G. Singh and other CSE employees would sometimes steal merchandise. A. Singh noted that G. Singh either sold such products himself, directed A. Singh to sell the products for a financial compensation, or directed A. Singh to ship the products to the California warehouse. According to A. Singh, in some cases, the theft was not necessarily intended from the outset, but was a by-product of the consolidation scheme. In these cases, products were sometimes unintentionally left behind at a CSE location during the process of commingling or separating loads. If CSE delivered the shipment before

realizing its mistake, it could not deliver the product left behind without revealing that it had opened the trailers that were purportedly sealed during the entire shipment. In such cases, G. Singh would direct that the product left behind simply remain at CSE and not be delivered. This was the case, A. Singh explained, with the L Brands pallets found at the CSE warehouse in Columbus, Ohio.

33. During another interview in March of 2022, A. Singh reported to law enforcement that while they worked together at CSE, G. Singh had directed him to sell stolen property, including the vacuums. A Singh reported that G. Singh kept some products for his personal use, sent some to the Kang brothers in California, and distributed some to G. Singh's relatives.

34. During the March 2022 interview, A. Singh also explained that G. Singh now operates Bhullar Transport from the PREMISES and other locations. A. Singh noted that G. Singh is still breaching seals, commingling loads, and stealing merchandise from sealed loads.

35. Text messages and photographs obtained from A. Singh's cell phone corroborate A. Singh's statements and revealed that from about January 2021 to March 2022, G. Singh has continued to breach seals and commingle loads in the new operation at the PREMISES. For example:

a) On or about February 22, 2021, a Bhullar Transport employee sent A. Singh a message that listed the company's address as 3739 Interchange Road, Columbus, OH 43228, one of the PREMISES addresses.

b) On or about August 03, 2021, a Bhullar Transport employee sent a message to a group of employees, including G. Singh. The message stated, "No load number on the bills also too much splits going on with mixed loads incorrect trailers on it as well no trailer pictures." Based on my training, experience, and a review of other related text

messages among these individuals, I understand the employee to mean that Bhullar Transport is breaching seals and commingling loads too often, which is leading to confusion and undelivered goods.

c) On or about August 13, 2021, a Bhullar Transport employee informed G. Singh and other employees that there were some pallets of product inadvertently left at the PREMISES, apparently during the process of separating and reconstituting commingled loads. G. Singh responded to the message, "Rinku have fun." A. Singh has told law enforcement that he was known as Rinku. Based on my training, experience, and a review of other related text messages among these individuals, I understand G. Singh to be directing A. Singh to handle the undelivered goods through potentially selling it.

d) On or about September 03, 2021, A. Singh sent an image of a bill of lading, which is a document describing the contents of a particular shipment, to a group of employees, including G. Singh. The bill of lading showed Bhullar Transport as the MC and reflected the following receiver note: "Received only 4plts NOT 5 plts." Based on my training, experience, and my review of the text messages, I understand this to mean that the recipient of a Bhullar Transport shipment stated that it received only four pallets of product when it was expecting five pallets.

e) On or about November 25, 2021, G. Singh informed a group of employees that Bhullar Transport's trailers numbered 543 and 287 were located at Bhullar Transport's yard. An employee of Bhullar Transport replied to G. Singh and others indicating that the load in Bhullar Transport's trailer 287 was transferred to Bhullar Transport's trailer W92087, and that trailer W92087 was at dock 4 with the bill of

lading and a new seal inside the trailer. Based on my training, experience, and my review of the text messages, I understand the Bhullar Transport employee to be telling G. Singh that a commingled load was being separated at the PREMISES. It appears that a shipment had been commingled with other shipments on trailer 287. According to the employee, one of the commingled shipments was then separated out from trailer 287 and placed on trailer W92087. Because the original seal on the shipment had been cut or broken during the commingling process, a new seal was being provided so that trailer W92087 could appear as if it had been sealed and never opened.

THE SUBJECT PREMISES

36. This investigation shows that evidence, fruits, and instrumentalities of the above mentioned crimes will be found at the PREMISES.

37. On or around February 12, 2021, G. Singh submitted an MCS-150 to the FMCSA on behalf of Bhullar Transport that listed the PREMISES as Bhullar Transport's principal place of business and mailing address where all the business-related documents were stored and maintained.

38. On August 18, 2021, G. Singh filed a "Statutory Agent Update" form with the Ohio Secretary of State, in which he listed the PREMISES as the address for Bhullar Transport's new statutory agent.

39. On March 02, 2022, A. Singh told law enforcement that the commingling and separating of loads was taking place at the PREMISES.

40. During a surveillance operation on March 24, 2022, a Special Agent from the USDOT-OIG witnessed Bhullar Transport trucks parked at the PREMISES. Additionally, on the

doors of the PREMISES were Bhullar Transport Group lettering and logos, which were also on the trucks parked at the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

41. As described above and in Attachment C, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. Because many of the records pertaining to MCs, CMVs, and shipping contracts are transferred or submitted electronically, and because G. Singh is known to communicate with his employees and potential co-conspirators via email and/or text message, your affiant has reason to believe that the records sought may be stored on a computer's hard drive, mobile devices, and other storage media located at the PREMISES. Furthermore, given the ubiquity and portability of mobile devices like cellular phones, your affiant also has reason to believe that the records sought may be stored on digital storage media located on the person of G. Singh. A storage medium is any physical object upon which computer data can be recorded. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools.

This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d) Based on actual inspection of other evidence related to this investigation, (e.g., email correspondence, binding estimates), I am aware that computer equipment was used to generate and store documents used in the scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

43. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b) As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or

controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may

indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

44. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

46. Bhullar Transport is a functioning company that conducts business. The seizure of Bhullar Transport's computers may limit its ability to conduct its legitimate business. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of Bhullar Transport so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

CONCLUSION

47. Based on the facts set forth above, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 659 (Theft from Interstate Shipment; 1001 (False Statement); 1343 (Wire Fraud); and 18 U.S.C. § 1349 (Wire Fraud Conspiracy) exist for the person of Gurtej Singh and the PREMISES. I therefore request that the Court issue a search warrant directing agents to conduct a search of G. Singh and the PREMISES, located at the above mentioned address, as further described in Attachments A and B for the items described in Attachment C.

BILAL TEMSAH Digitally signed by BILAL TEMSAH
Date: 2022.05.23 20:40:08 -04'00'

SPECIAL AGENT BILAL TEMSAH
U.S. DOT OIG

Subscribed and sworn to before me this 27th day of May, 2022.

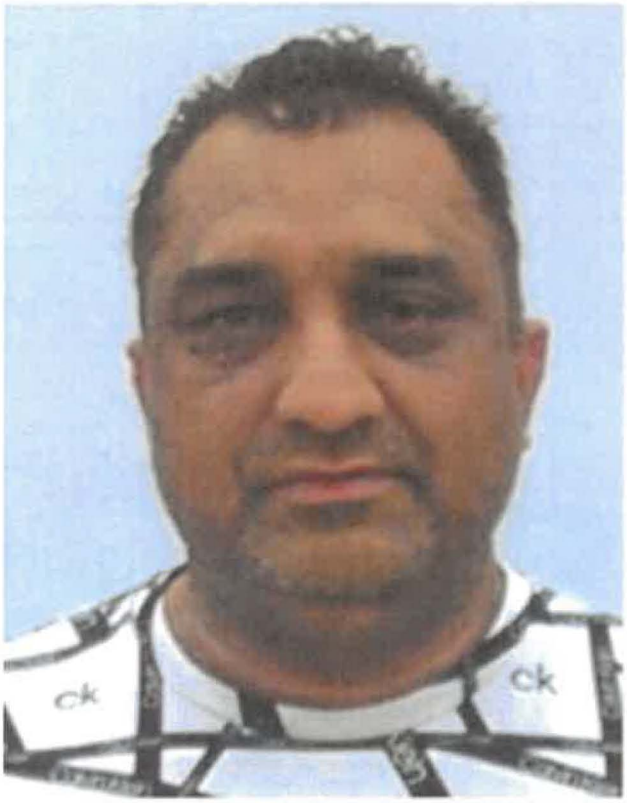
ELIZABETH A. PRESTON DEAVERS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A – DESCRIPTION OF PREMISES

Bhullar Transport Group (hereinafter referred to as "Bhullar Transport") is a business located at **3739 and 3743 Interchange Road, Columbus, OH 43204**. Bhullar Transport is located in an industrial building with units 3707 to 3743 Interchange Road Columbus, OH located in the building. The building is a white and grey stucco with a flat roof. The main entrance doors to various suits including 3739 and 3743 Interchange Road Columbus, OH, are located at the west side of the building. The front door to 3739 Interchange Road, Columbus OH 43204 has "Bhullar Transport Group LLC" lettering and the front door to 3743 Interchange Road, Columbus OH 43204 has a decal on it with the letter "B" in the middle of the decal. On the door for the 3739 suite there is a piece of paper that has "please see us @ the next door" with an arrow pointing toward the 3743 suite. On the east side of the building there appear to be at least two-bay doors and one steel entrance door. The steel door has the same decal that is on the front door of the 3743 suite. There were also two semi-trucks parked in the rear east side of the building that displayed decals for Bhullar Transport that was identical to the decal displayed on the 3743 suite door. The suites are the two most northern suites in the building.

ATTACHMENT B
PERSON TO BE SEARCHED

Gurtej Singh is a Black male having a date of birth of July 18, 1975 with black hair and brown eyes, standing approximately 5'11" tall, and weighing approximately 220 pounds. Singh is pictured below.



Gurtej Singh

ATTACHMENT C - ITEMS TO BE SEIZED

All records and information relating to violations of 18 U.S.C. § 1001 (False Statement); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. 659 (Theft from Interstate Shipment); and 18 U.S.C. § 1349 (Wire Fraud Conspiracy); those violations involving the financial or business affairs of Bhullar Transport, Showtime Carrier, Inc., Roadhawk Transport, and Cargo Solution Express (CSE), and Gurtej Bhullar Singh, also known as Gary Singh and Gary Bhullar, for the period of May 21, 2015 to the present. This specifically includes, without limitation:

a. Smartphones or cellular telephones, computers, and other digital media or digital storage devices.

b. Records and information showing ownership and control of Bhullar Transport and other motor carrier companies for which Gurtej Singh was an owner, manager, or otherwise held a position of supervisory control, including but not limited to the following:

    1. corporate minutes, agreements, contracts, filings, and correspondence reflecting, relating to, or concerning the Federal Motor Carrier Safety Administration (FMCSA), United States Department of Transportation (USDOT), or various Secretaries of State, including but not limited to California and Ohio; and

    2. Records, documents, and information tending to establish the identity of persons in control of the premises, including but not limited to utility bills and receipts, rental receipts, canceled mail envelopes, identification and/or travel documents, and other items which establish personal identification.

c. Records, documents, and information, including correspondence (in any form), relating to the shipping business activities of Bhullar Transport and other motor carrier companies for which Gurtej Singh was an owner, manager, or otherwise held a position of supervisory control, including but not limited to, rate confirmations, bills of lading, seal numbers, trailer inventories, contracts, sales agreements, invoices, claims, rejected loads, and other documents and communications, whether in draft or final form, concerning current or previously received requests or inquiries for any customer, shipper, broker, or receiver.

d. Payment information for transportation services provided by Bhullar Transport and other motor carrier companies for which Gurtej Singh was an owner, manager, or otherwise held a position of supervisory control, including financial records or documents, spreadsheets, records of payments, records of accounts payable and

receivable, letters of credit, credit card invoices or authorization, bank checks, wire transfers.

e. Tax returns, IRS filings, financial statements, and any related work papers.

f. All records and information related to personnel files containing, but not limited to, time cards, timesheets, payroll sheets, benefits paid, check stubs, jobs worked on, relating to current and former employees.

g. All records and information tending to show the identities of any co-conspirators.

All of the above-noted records may be stored on magnetic or electronic media including hard drives, diskettes, tapes, or other media in the form readable by a computer. These records include media maintained as an archive or backup copies. Also included in magnetic or electronic media are electronic data processing and storage devices, computers, and computer systems including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disks and diskettes, tape drives, and tapes, optical storage devices such as keyboards, printers, video display monitors, optical readers, and related communication devices such as modems. Computer equipment, as needed, is defined as follows:

a. Hardware. Computer hardware consists of all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but it not limited to, any data processing devices; internal and peripheral storage devices; input/output devices (such as keyboards, printers, scanners); related communication devices (such as modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Software. Computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital forms. It commonly includes programs to run operating systems, applications, utilities, compilers, interpreters, and communication devices.

c. Documentation. Computer-related documentation consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure hardware, software, or related items.

d. Handwritten or printed notes regarding passwords, finding the file or directory names of important data, operating the hardware or software, identifying the suspect's electronic or telephone connections with co-conspirators and victims, or finding login names or accounts.

For any computer, cell phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cell phone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER'S Internet activity, including firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).